ABSTRACT OF THE DISCLOSURE

A method and an apparatus ensuring protection of digital data are provided.

In addition to re-encrypting the data using an unchangeable key, the data is double re-encrypted using a changeable key. The changeable key is used first and the unchangeable key is then used, or in another case, the unchangeable key is used first, and the changeable key is then used. In the aspect of embodiments, there is a case adopting a software, a case adopting a hardware, or a case adopting the software and the hardware in combination. The hardware using the unchangeable key developed for digital video is available. In adopting the software, encryption/decryption is performed in a region below the kernel which cannot be handled by the user to ensure the security for the program and for the key used. More concretely, encryption/decryption is performed with RTOS using a HAL and a device driver, i.e., a filter driver, a disk driver and a network driver, in an I/O manager. Either one of two filter drivers, with a file system driver between them, may be used. Further, both filter drivers may be used.

世界知的所有権機関
国際事務局

PCT

特許協力条約に基づいて公開された国際出願

(51) 国際特許分類7 **H04L 9/14, G11B 20/10, H04N 7/167, G06F 17/60**	**A1**	(11) 国際公開番号	**WO00/22777**
		(43) 国際公開日	2000年4月20日(20.04.00)

(21) 国際出願番号 PCT/JP99/05704

(22) 国際出願日 1999年10月15日(15.10.99)

(30) 優先権データ
特願平10/309418 1998年10月15日(15.10.98) JP

15-Apr-01/30 mo

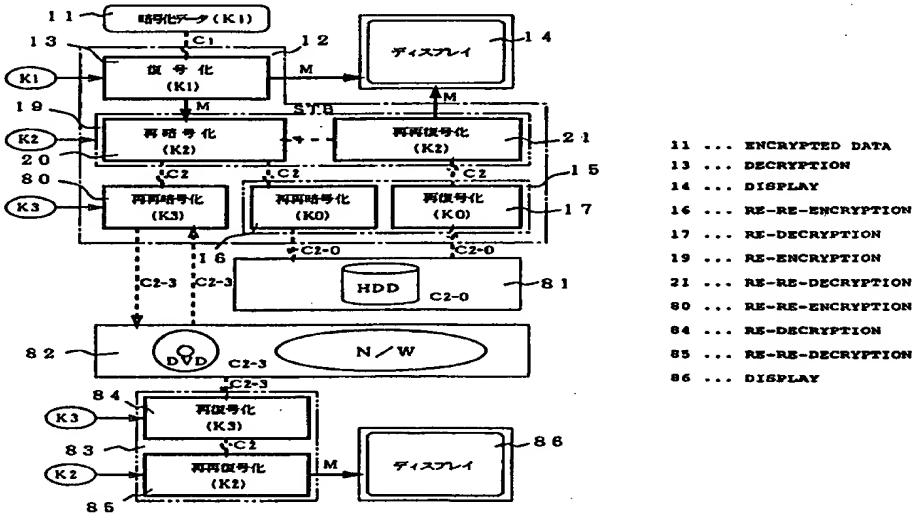
(71) 出願人（米国を除くすべての指定国について）
三菱商事株式会社(MITSUBISHI CORPORATION)[JP/JP]
〒100-8086 東京都千代田区丸の内二丁目6番3号 Tokyo, (JP)
(72) 発明者；および
(75) 発明者／出願人（米国についてのみ）
斉藤 誠(SAITO, Makoto)[JP/JP]
〒206-0012 東京都多摩市貝取2-12-6-104 Tokyo, (JP)
(74) 代理人
南條眞一郎(NANJO, Shin-ichiro)
〒101-0053 東京都千代田区神田美土代町7 南條特許事務所
Tokyo, (JP)

(81) 指定国 AE, AL, AM, AT, AU, AZ, BA, BB, BG, BR, BY, CA, CH, CN, CR, CU, CZ, DE, DK, DM, EE, ES, FI, GB, GD, GE, GH, GM, HR, HU, ID, IL, IN, IS, JP, KE, KG, KP, KR, KZ, LC, LK, LR, LS, LT, LU, LV, MD, MG, MK, MN, MW, MX, NO, NZ, PL, PT, RO, RU, SD, SE, SG, SI, SK, SL, TJ, TM, TR, TT, TZ, UA, UG, US, UZ, VN, YU, ZA, ZW, 欧州特許 (AT, BE, CH, CY, DE, DK, ES, FI, FR, GB, GR, IE, IT, LU, MC, NL, PT, SE), OAPI特許 (BF, BJ, CF, CG, CI, CM, GA, GN, GW, ML, MR, NE, SN, TD, TG), ARIPO特許 (GH, GM, KE, LS, MW, SD, SL, SZ, TZ, UG, ZW), ユーラシア特許 (AM, AZ, BY, KG, KZ, MD, RU, TJ, TM)

添付公開書類
国際調査報告書

(54)Title: METHOD AND DEVICE FOR PROTECTING DIGITAL DATA BY DOUBLE RE-ENCRYPTION

(54)発明の名称 2重再暗号化によりデジタルデータを保護する方法及び装置



(57) Abstract

A method and a device capable of protecting digital data reliably. Digital data are doubly re-encrypted by using a fixed key and a variable key. The order of using the encrypting keys is first the variable key and then the fixed key, or first the fixed key and then the variable key. The working examples are exemplified by one using a software, one using a hardware and one using a combination of a software and a hardware. The hardware can use a fixed key which has been developed for digital video. The software performs encryption/decryption in a region other than a kernel portion which cannot be used by the user so as to keep the safety of the program and the key used. Specifically, the encryption/decryption are performed by a filter driver in an I/O manager, a device driver serving as a driver/net driver and an RTOS utilizing an HAL. Either or both of two filter drivers on both sides of a file system driver can be use